Policy:	**1165**	**Effective:**	**12/06/06**
Procedure:	**1165.01**	**Replaces:**	**1165.01, 1165.02, & 1165.03**
Chapter:	**Investigations and Inspections**	**Dated:**	**03/22/00**
Rule:	**Arizona Criminal Justice Information System (ACJIS) Operations**		

Purpose:

Arizona Department of Juvenile Corrections (ADJC) accesses the Arizona Department of Public Safety's (DPS) Arizona Criminal Justice Information System (ACJIS)/ National Criminal Information Center (NCIC) system to conduct background clearances on new employees, visitors, maintenance/ construction contractual employees, volunteers, and also to enter/cancel warrants on juveniles who have violated provisions of conditional liberty. The System Security Officer or designee shall ensure that ACJIS information is held confidential and is accessed only for bona fide criminal justice or law enforcement needs.

Rules:

1. ACJIS system operations shall be under the supervision and control of the ADJC Investigations Chief Administrator:
   a. The **ADJC DIRECTOR OR DESIGNEE** shall appoint an ACJIS System Security Officer (SSO) in accordance with ACJIS and National Criminal Information Center (NCIC) rules and applicable statutes.

2. The **SSO** shall
   a. Oversee the administration and use of the ACJIS network by ADJC;
   b. Designate ACJIS operator(s) for Central Office;
   c. Enforce ACJIS system security by ensuring that ACJIS operating policies and procedures are followed;
   d. Ensure that ADJC is, at all times, in compliance with all ACJIS, ACIC, and NCIC rules and applicable statutes, including the certification of ACJIS network operators;
   e. Be responsible for all changes concerning the equipment connected to the ACJIS network and act as the liaison between ADJC Management Information Systems (MIS) and Department of Public Safety (DPS);
   f. Perform internal audits on a monthly basis in order to ensure ADJC compliance with all applicable rules, statutes, and required ACJIS response times;
   g. Complete Monthly Internal Audit Reports and forward to the Investigations Chief Administrator for review and corrective action, as needed;
   h. Complete specific administrative and coordinating responsibilities in relation to the ACJIS Network Operator Certification Program that include the following:
      i. Attend training provided by the DPS Access Integrity Unit and attend meetings held by the user advisory group;
      ii. Review and approve/disapprove applications for ACJIS operators and ACJIS Criminal Justice Practitioners to meet state and federal regulations regarding ACJIS training and access;
      iii. Determine certification levels that apply to ADJC personnel;
      iv. Submit to the DPS Access Integrity Unit a list of all ADJC ACJIS network operators indicating their respective names, dates of birth, agency identification, level of certification, and date of hire or assignment.
         (1) The **SSO** shall keep this list updated when any changes occur, including chief executive officer (CEO) and SSO changes.

v. Review and edit a semi-annual report (April, November) of all certified staff and the corresponding certification levels. Changes, additions, deletions shall be noted on the list;
vi. Ensure the certification test(s) are administered to agency personnel within six months of the operator's date of hire or assignment;
vii. Ensure proficiency training of operators;
viii. Ensure that all ACJIS network operators are certified within six months of their assignment as terminal operators and that all certified operators are re-tested within 30 days of the expiration of their current certification;
ix. Conduct or assign a designee to conduct certification tests for ACJIS network operators moving to a higher level of certification within 30 days after the date of the change/assignment;
x. Maintain copies of ACJIS Network Operator certificates at ADJC Central Office for audit purposes;
xi. Submit written notification to the DPS Access Integrity Unit within 15 days of an incident involving a lost or destroyed certificate;
xii. Ensure that in-depth training is provided to agency personnel who have failed the ACJIS Network certification testing, at most, three times.
    (1) Any employee who fails the fourth test shall not access/use the ACJIS/NCIC terminal equipment.
xiii. Submit a written request to the DPS Access Integrity Unit for extensions of certification/re-certification dates outlining the reasons for the extension requests;
xiv. Submit requests for training and/or training schedule changes in writing to the DPS Access Integrity Unit;
xv. Ensure that all ACJIS and NCIC manuals are updated and shared with the network operators as information is received including training material;
xvi. Submit the signature log (training) to the DPS Access Integrity Unit semiannually in April and November;
xvii. Ensure the integrity and security of the ADJC ACJIS services and related confidential materials;
xviii. Provide training on privacy and security issues to all users, including agency personnel categorized as criminal justice practitioners;
xix. In conjunction with DPS, coordinate the attendance of training provided by the access integrity unit and meetings held by the user advisory group;
xx. Participate in any ACJIS/NCIC Surveys on behalf of ADJC;
xxi. Ensure that all personnel authorized to receive information directly or indirectly have viewed the ACJIS operations overview tapes and assure that the video tape log is accurate and up to date;
xxii. Ensure that all administrative messages received via ALETS or NLETS are responded to in the required manner and appropriate time frame;
xxiii. Ensure that all hit confirmations are confirmed in the required manner and time frame;
xxiv. Ensure that validations are performed in the appropriate manner and within the required deadline;
xxv. Responsible for distributing to affected personnel all NCIC and ACJIS manual updates, newsletters; information bulletins and training and testing materials;
xxvi. Responsible for all changes concerning the equipment connected to the ACJIS network;
xxvii. Ensure that all background checks conducted using the ACJIS network are in compliance with ACJIS procedure and the records are maintained in a secured manner.

3. **ONLY AUTHORIZED ADJC EMPLOYEES** shall access the ACJIS network and only for lawful and bona fide purposes, including:

a. Performing criminal history investigations on personnel entering or working in ADJC secure facilities;
b. Entering and maintaining arrest warrant data;
c. Responding to inquiries regarding arrest warrants and other bona fide requests for assistance from ACJIS network users;
d. Performing ACJIS operations that support criminal investigations requested by the ADJC Investigations Division Investigators.

4. The **INSPECTIONS AND INVESTIGATIONS DIVISION (IID) CHIEF ADMINISTRATOR** shall ensure that the ACJIS network is established and maintained at Central Office IID, Adobe Mountain School (AMS), Black Canyon School (BCS), Catalina Mountain School (CMS), and Eagle Point School (EPS).

5. Adobe Mountain School is the Central Communications Center for ADJC and the **SECURITY CAPTAIN** shall ensure authorized ACJIS network operators are available 24 hours a day.

6. Each facility shall have an ACJIS Liaison who shall have the same responsibilities of the ADJC System Security Officer pertaining to ACJIS operations at the facilities.
   a. Each secure facility **SECURITY CAPTAIN** shall designate employees to be ACJIS operators;
   b. The **SECURITY CAPTAIN FROM EACH FACILITY IN CONSULTATION WITH THE SYSTEM SECURITY OFFICE** shall designate certified ACJIS network operators to act as the facility ACJIS Liaison. The facility **ACJIS LIAISON** shall:
      i. Act as contact persons between the Agency Captain and the ACJIS Operators with regard to any questions, problems, or concerns related to the use or operations of ACJIS;
      ii. Maintain ACJIS manual and computer disk updates;
      iii. Ensure the security and maintenance of the ACJIS manuals, equipment, information, or products.

7. The **SSO** shall certify selected personnel to access the ACJIS network and equipment and to have access to and review information obtained through ACJIS. The agency **SSO** certifies three different levels of access authorization:
   a. Level A is the highest access level and shall be authorized only for those individuals who have a bona fide job-related need. These ACJIS operators enter records into the ACIC/NCIC, as well as modify, clear, cancel, and/or locate records. These operators also inquire into the ACJIS/NCIC network and interpret responses.
      i. **LEVEL A OPERATORS** shall successfully complete a 100 item certification test that shall not exceed three hours.
   b. Level B network operators inquire into the ACJIS/NCIC network and interpret answers only. These operators shall not enter or update record entries.
      i. **LEVEL B OPERATORS** shall successfully complete a 50 item certification test that shall not exceed two hours.
   c. Level C operators have a limited inquiry access. These operators shall only access the ACJIS/NCIC "hot files" through a Mobile Digital Terminal (MDT).
      i. **LEVEL C OPERATORS** shall successfully complete a 25 item certification test that shall not exceed one hour.
   d. Criminal Justice Practitioner (CJP) has been approved to review and have access to information obtained through ACJIS. The **CJP** shall not access the ACJIS/NCIC network. The **CJP** shall view security and privacy training video tapes.
      i. The training shall address security and privacy issues concerning any information obtained via the ACJIS/NCIC network:
         (1) CJP training shall include only those employees needing access to information obtained via the ACJIS network;

(2) Upon completion of training, the **CJP** shall sign a log which verifies his/her participation in the training exercises and the viewing of training video tapes;
(3) The agency **SSO** shall maintain the training log for a six month period. In April and November, the agency **SSO** shall submit these logs to the DPS Access Integrity Unit.

8. Use of the ACJIS network, or any information obtained from ACJIS, shall be for bona-fide law enforcement and criminal justice purposes ONLY. SECONDARY DISSEMINATION OF ANY ACJIS INFORMATION IS STRICTLY PROHIBITED.

9. The data available through ACJIS is documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. Information obtained from ACJIS sources is controlled by various Federal and state privacy laws, as well as general policy dictated by the Federal Bureau of Investigation. The use of ACJIS or any ACJIS information for billing, civil process, risk management, curiosity, or for personal reasons is strictly prohibited:
   a. Any **INDIVIDUAL WHO OBTAINS INFORMATION THROUGH ACJIS FOR A PROHIBITED PURPOSE OR WHO IMPROPERLY DISSEMINATES INFORMATION** obtained through ACJIS shall be subject to administrative discipline up to and including dismissal, as well as criminal and/or civil prosecution;
   b. Access to the ACJIS network or any information obtained through the ACJIS network is restricted to authorized operators and approved Criminal Justice Practitioners;
   c. Computers with access to the ACJIS network, manuals and/or computer disk manuals, shall be located and secured. Only those individuals authorized by this procedure may have access to the physical area and/or any ACJIS information;
   d. Only Level A or Level B ACJIS operators shall have access to the ACJIS network;
   e. **CERTIFIED ACJIS OPERATORS** shall not perform any function above their current level of certification.

10. An **EMPLOYEE SEEKING CERTIFICATION** as an ACJIS network operator shall submit Form 1165.01A, "Request for Access To Arizona Criminal Justice Information System", through the chain of command
   a. The **FACILITY CAPTAIN OR DESIGNEE** shall submit approved training requests approved to the ADJC System Security Officer for final review and approval/denial.
      i. The **ADJC SSO** is responsible for ensuring (to DPS and federal authorities) that the approved trainees' job responsibilities necessitate ACJIS access;
   b. The **ADJC SSO** coordinates training for approved ACJIS network operator candidates;
   c. The **FACILITY ACJIS LIAISON AND/OR DESIGNEE** shall ensure the network operators knowledge by observing the operator's hands-on proficiency:
      i. Test record entries are available for training purposes and are listed in the TOC Instructor Manual data base;
      ii. After successfully completing training and testing, the candidate is awarded a certificate by DPS designating eligibility for either Level A or Level B ACJIS access;
   d. The **ADJC SYSTEM SECURITY OFFICER** shall obtain a certification number (TOC) for the network trainee prior to giving them authority to access the system.
      i. A trainee's interim authority shall automatically cease when the ACJIS operator is certified or six months of training time has elapsed, whichever comes first.
         (1) ACJIS Network Experience: Once assigned a TOC number, an **ACJIS OPERATOR** may work at least one (1) month (and no more than 6 months), performing routine ACJIS network access under the supervision of a certified operator.
   e. A **CERTIFIED ACJIS OPERATOR WHO REQUESTS RE-CERTIFICATION** at a higher level of access must satisfactorily pass the written and practical examinations within 30 days of commencing training for the higher level certification.

i. Certification as an ACJIS operator automatically expires two years from the date of issuance of the certificate.

f. **CERTIFIED ACJIS OPERATORS** shall request re-certification and satisfactorily pass the required written examination at least 30 days prior to the expiration of their certificate.
   i. **ACJIS OPERATORS WHOSE CERTIFICATES EXPIRE** shall cease to act as operators until re-certified.

g. Changing Employment/Reinstatement*:* TOC numbers and certificates are assigned to individual ACJIS operators and are not reassigned or reissued. A change in employment status does not affect the certificate or issued TOC number. Both are retained by the individual terminal operator. The **ACJIS OPERATOR** shall inform the ADJC System Security Officer of such changes.

Effective Date:	Approved by Process Owner:	Review Date:	Reviewed By:
11/29/06	John Dempsey		